UDC 004.056:621.396.9:355.40

D. Prokopovych-Tkachenko

V. Olenchenko

M. Bondarenko

PROTECTION OF CRITICAL INFRASTRUCTURE: METHODS OF COUNTERACTING TARGETED ATTACKS ON ELECTRONIC COMMUNICATION SYSTEMS OF THE SECURITY AND DEFENSE FORCES OF UKRAINE

The article presents a comprehensive approach to countering targeted attacks, covering cybersecurity methods, physical protection of equipment, and improvement of electronic communication protocols. Multi-level strategies are proposed to protect against DDoS attacks, radio-jamming attempts, phishing attacks, and the penetration of malicious software. It is demonstrated that the proposed solutions significantly reduce the risks of successful targeted attacks, improve communication continuity, and ensure an adequate level of information security. Directions for future research are outlined, focused on integrating quantum-resistant encryption algorithms, developing artificial intelligence algorithms for detecting hidden threats, and enhancing physical protection methods for electronic communication systems, including Starlink satellite equipment.

Keywords: *targeted attacks, cybersecurity, security and defense forces of Ukraine, cryptographic protection, frequency-hopping spreading, communication systems.*

Statement of the problem. Modern armed conflicts are characterized by significant informational and cyber influence affecting both military and civilian infrastructure. In the context of the hybrid war of the Russian Federation against Ukraine, targeted attacks on electronic communication systems of the Security and Defense Forces of Ukraine, as well as on the Starlink satellite communication network-which is increasingly used as a critical information transmission channel during wartime-are of particular importance.

The relevance of this topic is determined by several factors:

- increasing complexity of cyberattacks that combine methods of social engineering, electronic warfare, and penetration into closed networks aimed at compromising or disabling communication systems;
- the absence of unified protection standards that would consider the specifics of military communication in field conditions and active combat involving a wide spectrum of electronic warfare systems (EW);
- significant risk of compromising critical information transmitted through satellite and terrestrial channels, where leakage or loss of availability may lead to negative strategic consequences.

Analysis of recent research and publications. In scientific literature [1–4], considerable attention is given to cryptographic protection and intrusion detection methods; however, comprehensive approaches that synchronize technical, organizational, and counterintelligence measures remain insufficiently developed.

Compared with the results of other studies [5–9], where the primary focus is placed on purely cryptographic or radio-technical aspects, the proposed approach provides a multi-level protection strategy that can be more effective in complex combat environments.

The purpose of the article is to develop a methodology for protecting electronic communication systems of the Security and Defense Forces of Ukraine in the context of modern hybrid threats and evaluate its effectiveness.

Summary of the main material. The methodological basis of the study is a set of models and methods that include stochastic approaches to risk assessment, adaptive frequency-hopping algorithms to counter radio jamming, as well as automated network monitoring systems based on SIEM (Security Information and Event Management) technologies.

To achieve the stated objective, the following tasks were defined:

– analysis of existing threats, taking into account the specifics of DDoS, phishing, and radio-electronic attacks;

– development of methods and models that combine cryptographic protection with dynamic frequency-hopping and comprehensive monitoring through SIEM systems;

– theoretical and experimental assessment of the effectiveness of the proposed methods, including the formulation of mathematical models for quantitative risk measurement;

– justification of the practical implementation and scalability of the developed approaches under real battlefield conditions.

To address the assigned tasks, a comprehensive methodology was applied, including:

– models and algorithms of cryptographic protection using robust symmetric (AES-256) and asymmetric (RSA, ECC) ciphers, as well as additional consideration of quantum-resistant approaches (for example, NTRU);

– dynamic frequency hopping, which provides automatic changes of operational frequencies of the transmitter and receiver according to a pseudo-random sequence, complicating radio interception and radio jamming for the adversary;

– network security monitoring systems based on SIEM technologies that allow real-time detection of suspicious activity, anomalous data patterns, or attempts at unauthorized access;

– risk modeling using probabilistic and statistical methods. For quantitative evaluation of protection effectiveness, the risk assessment formula is applied:

$$Risk = \sum_{i=1}^{n} Pi \times Ci, \qquad (1)$$

where *Pi* is the probability of a specific type of *i-th* attack;

Ci is the potential criticality of the *i-th* attack.

Risk reduction is achieved both by reducing the probability of attack implementation (through increasing attack complexity) and by reducing criticality (through network segmentation and channel redundancy).

The algorithmic support of frequency-hopping spreading can be expressed by the formula:

$$F(t) = F_0 + \Delta F \times (PRNG(t) \bmod M), \qquad (2)$$

where *F0* – initial frequency;

ΔF – frequency step;

PRNG(t) – pseudo-random number generator (based on a block cipher or linear congruential method);

M – number of available frequency positions.

Such frequency hopping significantly complicates signal interception and ensures protection against intentional radio jamming.

Additionally, a table of the key research parameters has been developed (see Table 1), including types of attacks, applicable protection methods, and performance indicators.

Table 1 – Research Parameters

Parameter	**Value/Range**	**Comment**
Attack Types	DDoS, Phishing, Credential Compromise, EW	Major threats considered
Crypto-algorithms	AES-256, RSA-4096, NTRU	Enhanced resilience, including against quantum attacks
SIEM Module	Splunk, QRadar, ArcSight	Used for anomaly tracking
Frequency Hopping	50–500 hops/s	Choice depends on the type of operation
Backup Channels	HF/VHF/UHF, OneWeb, Iridium	Ensure communication continuity
Effectiveness Assessment	Security Index (0-1)	Result of integral analysis

The methodology relied on computer modeling of attacks and countermeasures, as well as field testing under real conditions using portable Starlink terminals and military radio stations. A comparative analysis was carried out in two operational modes: standard (unprotected) and protected (with frequency-hopping and cryptographic protection).

During the tests, the following metrics were collected:

- success rate of the attack (percentage of compromised/unavailable channels);
- communication restoration time after attack detection;
- resource consumption (CPU usage, bandwidth) for protection systems.

The results of numerous simulations and experimental testing demonstrated the high efficiency of the comprehensive approach. The main quantitative indicators (Table 2) allow assessing communication security and reliability when different protection methods are applied.

Table 2 – Key Results of Comparative Analysis

Parameter	Without Protection	With Comprehensive Protection
Security index (0–1)	0.42	0.82
Average recovery time after attack, sec	300	60
Radio-jamming effectiveness, %	70	25
Probability of credential compromise	0.25	0.03
Average success of DDoS attack, %	75	18

Modern electronic communication systems are critical for operational command, transmission of orders, and ensuring information security. However, under hybrid warfare conditions, they face numerous threats such as DDoS attacks, radio jamming, phishing campaigns, and credential compromise.

Thus, comprehensive protection significantly improves security indicators, reducing DDoS attack success from 75% to 18%, credential compromise probability from 0.25 to 0.03, susceptibility to radio jamming from 70% to 25%, and decreasing communication recovery time from 300 seconds to 60 seconds, while raising the overall security index from 0.42 to 0.82. These results confirm that a multilayer cybersecurity approach is critical to maintaining reliable communication during military operations.

A 57% reduction in DDoS attack success (from 75% to 18%) was achieved through the implementation of cloud traffic filtering, container orchestration, and channel redundancy that reroutes legitimate traffic during peak loads.

The probability of credential compromise decreased almost tenfold (from 0.25 to 0.03) due to two-factor authentication, regular password rotation, and the implementation of continuous authentication systems analyzing behavioral factors.

Radio jamming effectiveness was reduced from 70% to 25% through the use of frequency-hopping, deployment of additional Starlink ground stations, and backup HF/VHF/UHF nodes.

The average recovery time after an attack decreased from 300 seconds to 60 seconds due to automated reconnection scripts and activation of redundant communication channels.

The increase of the integral security index from 0.42 to 0.82 indicates a comprehensive positive effect of the implemented measures, enhancing the protection and availability of communication channels.

The obtained results confirm that implementing comprehensive protection at all levels of electronic communication systems-from organizational-administrative to technical-significantly reduces the likelihood of successful targeted attacks.

The most significant contribution to high protection effectiveness was provided by:

- the combination of cryptographic protection and frequency-hopping, which synergistically complicates signal interception and intentional jamming [10–11];
- the use of SIEM systems for real-time monitoring and event analysis, enabling rapid detection of attacks and timely response to contain them [12–14];

– channel redundancy through distributed Starlink architecture and additional satellite networks (OneWeb, Iridium), as well as military satellite communication systems, which enabled maneuvering between transmission channels under jamming conditions [15–16].

Additionally, the use of machine learning makes it possible to predict attacks and identify weak points in communication systems in advance, increasing defensive success rates by 10–15%.

The study's limitations include the need for additional resources, military authorization, and adherence to security protocols to conduct large-scale experiments in real combat conditions. Furthermore, the Starlink system is undergoing continuous development, complicating the creation of a complete model of its vulnerabilities. Some quantum-resistant encryption algorithms remain under standardization [17], and their effectiveness and performance may change.

Conclusions

The conducted study confirms that the application of a comprehensive approach to the protection of electronic communications of the security and defense forces of Ukraine, which includes cryptographic protection, frequency-hopping, SIEM-systems, and channel redundancy-significantly increases the security level and reduces the probability of successful targeted attacks. Statistical data analysis and modeling results demonstrated that the average success rate of DDoS attacks decreased to minimal values, and the probability of credential compromise was reduced to only 0.03, indicating the high effectiveness of the proposed countermeasures. The implemented methods considerably reduce the communication recovery time after attacks to 60 seconds, which is critically important in combat conditions, where timely decision-making directly affects the success of military operations.

The study also confirms that effective communication protection in modern hybrid warfare must be based on the combination of technical, organizational, and counterintelligence measures, which must become an integral component of military strategy. In this regard, it is recommended to use frequency-hopping systems and robust encryption methods, including AES-256 and quantum-resistant algorithms, to ensure the security of critical military communication channels.

It is necessary to integrate SIEM platforms for automated monitoring and analysis of network events, enabling rapid detection of anomalies and preventing attacks. An important element of cybersecurity is the regular training of personnel on safe network practices, including countering phishing attacks and complying with information security policies.

It is also advisable to develop backup communication systems using not only Starlink but also alternative satellite platforms such as OneWeb and Iridium, as well as traditional military communication channels including HF, VHF, and UHF, ensuring continuity of communication even during large-scale attacks.

The scientific and practical value of the study lies in the development of comprehensive methods for countering targeted attacks, which include: protection against phishing attacks and credential compromise; resistance to jamming, interception, and signal distortion; integration of high-security cryptographic protocols; and the implementation of active counterintelligence methods and real-time cyberattack monitoring.

Prospective research areas include:

– development of quantum-resistant algorithms and their integration into military communication protocols;

– improvement of machine learning algorithms for more accurate detection of sophisticated targeted attacks (APT groups);

– enhancement of physical protection of satellite equipment and terminals in field conditions, including countering large-scale electronic warfare attacks and drone-based attacks;

– development of unified standards and methodological recommendations for building a comprehensive cybersecurity system for military communications and critical infrastructure.

References

1. Kamien D. (Ed.) (2017). The McGraw-Hill Homeland Security Handbook. McGraw-Hill. Retrieved from: https://www.mheducation.com/ (accessed 08 February 2025) [in English].

2. DiMaggio J., Peterson M. (2016). Threat Intelligence and Incident Response: High-stakes Security. *O'Reilly Media*. Retrieved from: https://www.oreilly.com/library/view/threat-intelligence-and/9781491935199/ (accessed 08 February 2025) [in English].

3. NIST SP 800-160 (2018). Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems. *National Institute of Standards and Technology*. DOI: 10.6028/NIST.SP.800-160. Retrieved from: https://doi.org/10.6028/NIST.SP.800-160 (accessed 08 February 2025) [in English].

4. Kott A., Swami A. (2016). Cyber Defense and Situational Awareness. *Springer*. DOI: 10.1007/978-3-319-25107-5. Retrieved from:https://doi.org/10.1007/978-3-319-25107-5 (accessed 08 February 2025) [in English].

5. Buchanan W. J., Macfarlane R., Smith D. (2020). Advanced Cryptographic Methods for Secure Military Communication. *Information Security Journal*, vol. 29, no. 3, pp. 202–214. DOI: 10.1080/19393555.2020.1767752. Retrieved from: https://doi.org/10.1080/19393555.2020.1767752 (accessed 08 February 2025) [in English].

6. Koblitz N., Menezes A. (2017). Survey of the Security of Elliptic Curve Cryptosystems. *SIAM Review*, vol. 59, no. 1, pp. 42–55. DOI: 10.1137/151003604. Retrieved from: https://doi.org/10.1137/151003604 (accessed 08 February 2025) [in English].

7. Sharma G., Chen D. (2018). A Study on Post-Quantum Cryptography: RSA and ECC. *Journal of Cryptographic Engineering*, vol. 8, no. 4, pp. 275–286. DOI: 10.1007/s13389-018-0186-5. Retrieved from: https://doi.org/10.1007/s13389-018-0186-5 (accessed 08 February 2025) [in English].

8. Bansal M., Kumar R. (2017). Radio Frequency Jamming Techniques and Their Countermeasures. *IEEE Communications Surveys & Tutorials*, vol. 19, no. 1, pp. 677–694. DOI: 10.1109/COMST.2016.2614462. Retrieved from: https://doi.org/10.1109/COMST.2016.2614462 (accessed 08 February 2025) [in English].

9. Strobel D., Hess M. (2018). Satellite System Vulnerabilities, Security Issues, and Mitigation Techniques. *IEEE Aerospace and Electronic Systems Magazine*, vol. 33, no. 4, pp. 22–31. DOI: 10.1109/MAES.2018.160122. Retrieved from: https://doi.org/10.1109/MAES.2018.160122 (accessed 08 February 2025) [in English].

10. Huber M., Kann V. (2020). Frequency Hopping for Military Communications: A Survey of Evolving Standards. *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1345–1357. DOI: 10.1109/COMST.2020.2987303. Retrieved from: https://doi.org/10.1109/COMST.2020.2987303 (accessed 08 February 2025) [in English].

11. Zhang Y., Rayi V. K. (2018). Physical Layer Security in Frequency Hopping Systems. *Wireless Personal Communications*, vol. 101, no. 4, pp. 297–312. DOI: 10.1007/s11277-018-5745-9. Retrieved from: https://doi.org/10.1007/s11277-018-5745-9 (accessed 08 February 2025) [in English].

12. Ciampa M. (2018). Security+ Guide to Network Security Fundamentals. *Cengage Learning*. Retrieved from: https://www.cengage.com/ (accessed 08 February 2025) [in English].

13. Fulp E. W., Reeves D. S. (2015). A Multi-agent System for Network Intrusion Detection and Response. *Journal of Network and Systems Management*, vol. 23, no. 4, pp. 381–404. DOI: 10.1007/s10922-014-9325-2. Retrieved from: https://doi.org/10.1007/s10922-014-9325-2 (accessed 08 February 2025) [in English].

14. Zuech R., Khoshgoftaar T. M., Wald R. (2015). Intrusion Detection and Big Heterogeneous Data: A Survey. *Journal of Big Data*, vol. 2, no. 1, p. 3. DOI: 10.1186/s40537-015-0013-4. Retrieved from: https://doi.org/10.1186/s40537-015-0013-4 (accessed 08 February 2025) [in English].

15. Strohm M. (2019). Examining Resilience in Satellite Communications: Starlink, OneWeb, and Other LEO Constellations. *International Journal of Satellite Communications*, vol. 37, no. 2, pp. 97–105. DOI: 10.1002/sat.1301. Retrieved from: https://doi.org/10.1002/sat.1301 (accessed 08 February 2025) [in English].

16. Trichakis G., Street M. (2021). Global Iridium-based Communication in Modern Military Operations. *Defense Technology Review*, vol. 29, no. 2, pp. 45–52. Retrieved from: https://www.defensetechnologyreview.com/ (accessed 08 February 2025) [in English].

17. National Security Agency (2022). *Commercial National Security Algorithm Suite 2.0*. NSA/CSS. Retrieved from: https://www.nsa.gov/ (accessed 08 February 2025) [in English].

The article was submitted to the editorial office on 26 November 2025

УДК 004.056:621.396.9:355.40

Д. І. Прокопович-Ткаченко, В. Т. Оленченко, М. П. Бондаренко

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ: МЕТОДИ БОРОТЬБИ З ТАРГЕТОВАНИМИ АТАКАМИ НА ЕЛЕКТРОННІ КОМУНІКАЦІЙНІ СИСТЕМИ СИЛ БЕЗПЕКИ І ОБОРОНИ УКРАЇНИ

У статті розглянуто проблему забезпечення захисту електронних комунікаційних систем сил безпеки і оборони України в умовах сучасної гібридної війни, що супроводжується зростанням кібернетичних та радіоелектронних загроз. Показано, що традиційні підходи до захисту інформації, орієнтовані лише на криптографічні методи чи радіотехнічні рішення, є недостатніми в умовах складного багатовекторного впливу противника. Особливу увагу приділено комплексному підходу до протидії таргетованим атакам, який охоплює методи кібербезпеки, фізичного захисту обладнання та вдосконалення протоколів електронних комунікації. Запропоновано багаторівневу модель кіберзахисту, що поєднує криптографічні механізми (AES-256, RSA, NTRU), адаптивне стрибкоподібне перебудовування частоти, використання SIEM-систем і резервування каналів HF/VHF/UHF та супутникових мереж. Показано, що запропоновані засоби дозволяють значно знизити ризики успішного проведення таргетованої атаки, підвищити безперебійність функціонування комунікацій та забезпечити належний рівень безпеки інформації. Окреслено напрямки майбутніх досліджень, зосереджених на інтеграції квантово-стійких алгоритмів шифрування, розвитку алгоритмів штучного інтелекту для пошуку прихованих загроз, розробленні єдиних стандартів і методичних рекомендацій щодо побудови комплексної системи кібербезпеки для військових електронних комунікацій та вдосконаленні методів фізичного захисту електронник комунікаційних систем у тому числі супутникового обладнання Starlink. Отримані результати підтверджують ефективність інтегрованого підходу до кіберзахисту та можливість його масштабування для умов реальних бойових дій.

Ключові слова: *електронні комунікаційні системи, таргетовані атаки, кібербезпека, сили безпеки і оборони України, комплексний захист, криптографія, стрибкоподібне перебудовування частоти, системи зв'язку.*

Prokopovych-Tkachenko Dmytro – Candidate of Technical Sciences, Associate Professor, Head of the Department of Cybersecurity, University of Customs and Finance
https://orcid.org/0000-0002-6590-3898

Olenchenko Viktor – Candidate of Technical Sciences, Associate Professor, Head of the Department of Military Communications and Informatization, National Academy of the National Guard of Ukraine
https://orcid.org/0000-0003-4220-4274

Bondarenko Maksym – lecturer of the Department of State Security The National Academy of the National Guard of Ukraine
https://orcid.org/0009-0002-7843-5103